Basics of windows

Versions of Windows

Due to Windows irregular way of naming their operating systems it can be a bit hard to keep track on. So here is a list of the desktop OS, and then a list of Servers.

Windows desktops OS

```
 Operating System    Version Number

Windows 1.0                    1.04
Windows 2.0                    2.11
Windows 3.0                    3
Windows NT 3.1                 3.10.528
Windows for Workgroups 3.11    3.11
Windows NT Workstation 3.5  3.5.807
Windows NT Workstation 3.51    3.51.1057
Windows 95                     4.0.950
Windows NT Workstation 4.0     4.0.1381
Windows 98                     4.1.1998
Windows 98 Second Edition      4.1.2222
Windows Me                     4.90.3000
Windows 2000 Professional      5.0.2195
Windows XP                     5.1.2600
Windows Vista                  6.0.6000
Windows 7                      6.1.7600
Windows 8.1                    6.3.9600
Windows 10                     10.0.10240
```

Windows Server

```
 Windows NT 3.51                  NT 3.51
Windows NT 3.5                   NT 3.50
Windows NT 3.1                   NT 3.10
Windows 2000                     NT 5.0

    Windows 2000 Server
    Windows 2000 Advanced Server
    Windows 2000 Datacenter Server

Windows NT 4.0                   NT 4.0

    Windows NT 4.0 Server
    Windows NT 4.0 Server Enterprise
    Windows NT 4.0 Terminal Server Edition

Windows Server 2003              NT 5.2

    Windows Small Business Server 2003
    Windows Server 2003 Web Edition
    Windows Server 2003 Standard Edition
    Windows Server 2003 Enterprise Edition
    Windows Server 2003 Datacenter Edition
    Windows Storage Server

Windows Server 2003 R2           NT 5.2

    Windows Small Business Server 2003 R2
    Windows Server 2003 R2 Web Edition
    Windows Server 2003 R2 Standard Edition
    Windows Server 2003 R2 Enterprise Edition
    Windows Server 2003 R2 Datacenter Edition
    Windows Compute Cluster Server 2003 (CCS)
    Windows Storage Server
    Windows Home Server
    Windows Home Server

Windows Server 2008               NT 6.0

    Windows Server 2008 Standard
    Windows Server 2008 Enterprise
    Windows Server 2008 Datacenter
    Windows Server 2008 for Itanium-based Systems
    Windows Server Foundation 2008
    Windows Essential Business Server 2008
    Windows HPC Server 2008
    Windows Small Business Server 2008
    Windows Storage Server 2008
    Windows Web Server 2008

Windows Server 2008 R2            NT 6.1

    Windows Server 2008 R2 Foundation
    Windows Server 2008 R2 Standard
    Windows Server 2008 R2 Enterprise
    Windows Server 2008 R2 Datacenter
    Windows Server 2008 R2 for Itanium-based Systems
    Windows Web Server 2008 R2
    Windows Storage Server 2008 R2
    Windows HPC Server 2008 R2
    Windows Small Business Server 2011
    Windows MultiPoint Server 2011
    Windows Home Server 2011
    Windows MultiPoint Server 2010

Windows Server 2012               NT 6.2

    Windows Server 2012 Foundation
    Windows Server 2012 Essentials
    Windows Server 2012 Standard
    Windows Server 2012 Datacenter
    Windows MultiPoint Server 2012

Windows Server 2012 R2            NT 6.3

    Windows Server 2012 R2 Foundation
    Windows Server 2012 R2 Essentials
    Windows Server 2012 R2 Standard
    Windows Server 2012 R2 Datacenter

Windows Server 2016     2016       NT 10.0
```

Windows Networks

There are mainly two ways to structure a Windows network. One is using a server-client model called **Domain** and the other is through a peer-to-peer like model called **Worksgroup**.

Windows domain

On Windows domain all users are connected to a domain controller.

So when you log in to your machine it authenticates against the domain controller. This way it is ultimately the domain controller that decides security policy. Length of password, how often it should be changed, disabling accounts. If a users quits his/hers job you can just remove his/her account. The person in control over the domain controller is in control of the network. As a pentester you are most likely very interesting in gaining access the the domain controller with Administrator-privileges. That means you control the network.

Since you authenticate against a domain controller you can log in to your account from any of the machines in the network. Think of systems you have had in schools and universities, where you can just sit down by any computer and log in to your account. This is usually a domain type network.

In order to set up a Domain network you need at least one Windows server for the domain controller.

If you have hacked a machine and you want to know if it is part of either a Workgroup or a domain you can do the following: go to `Control panel/System`. If it says `Workgroup: something` it means that the machine is connected to a workgroup, and not a domain.

Active directory

From Windows 2000 and on the application **Active directory** has been program used for maintaining the central database of users and configurations.

Domain controller

Any windows computer can be configured to be a domain controller. The domain controller manages all the security aspects of the interaction between user and domain. There are usually a least two computers configured to be domain-controllers. In case one breaks down.

If you have compromised a machine that belong to a domain you can check if it has any users. DC:s don't have local users.

If you run enum4linux you can look out for this section

```
 Nbtstat Information
<1c> - <GROUP> B <ACTIVE>  Domain Controllers
```

A third way is to run this command

```
echo %logonserver%
```

SMB

On networks that are based on Linux and you need to integrate a windows machine you can use SMB to do that.

Kerberos

Kerberos is a network authentication protocol. The original protocol is used by many unix-systems. Windows have their own version of the Kerberos protocol, so that it works with their NT-kernel. It is used by windows Domains to authenticate users. But kerberos can also be found in several unix-operating systems. Kerberos was not built by windows, but long before.

I think a machine that has port 88 open (the default kerberos port) can be assumed to be a Domain Controller.

When a user logs in to the domain Active Directory uses Kerberos to authenticate the user. When the user insert her password it gets one-way encrypted and sent with Kerberos to the Active directory, which then compares it with its password database. The Key Distribution Center responds with a TGI ticket to the user machine.

Workgroup

A workgroup architecture stands in contrast to the domain-system. A workgroup is based on the idea of peer-to-peer and not server-client as domain is. In a domain network you have a server (domain controller) and a client (the user). Therefore it might be a bit hard to control a network bigger than a dozen clients. So it is usually used for smaller networks. If a computer is part of a workgroup it cannot be part of a domain. In a workgroup architecture each computer is in charge of its own security settings. So there is no single computer in charge of all the security settings for the workgroup. This is good because you don't have one single point of failure, bt is also bad because you have to trust the users to configure their machines securely.

In a network you can have several workgroups. But that is usually not the case.

In a workgroup users can see each other, and share files.

User privileges

How does the user-system work on windows.

System (user)

System is actually not a user per se. System is technically a security principle. One big difference between System and Administrator is that is the computer is connected to a domain the system user can access the domain in the context of the domain account. The administrator cannot.

On windows it is possible to grant permission of a file to System but not to Administrator.

One example of this is the SAM key, which contains local account information. The System user has access to this information, but the Administrator does not.

http://superuser.com/questions/504136/root-vs-administrator-vs-system

Administrator

Administrator is a default account on Windows. It is the user with the highest privileges.

Normal user

The normal user obviously have less privileges than the Administrator.

You can add a new user through the cmd with the following command:

```
 net user username /add
net user kalle secret_password123 /add

# Add user to administrator group - thus making it administrator
net localgroup administrators kalle /add

# Add to Remote Desktop User
https://www.windows-commandline.com/add-user-to-group-from-command-line/
```

Structure of windows

https://en.wikipedia.org/wiki/Directory_structure

Windows 7

The root folder of windows `c:\` by default contains the following

```
 Windows
Users
```

Registry

You often hear talk about the registry when talking about Windows. But what is really the registry?

Well the windows registry is a hierarchical database that stores low-level settings used by the OS or any other application that uses it. The SAM (Security account manager) uses it, along with a lot of other stuff.

There is not really any equivalent for the Registry in Linux. Most configurations are done in text-files in Linux.You can usually find the under `/etc`.

Edit the registry

In Linux you usually just sudo-edit a config-file in `/etc`. In Windows you open Regedit and you can see the whole hierarchy. The registry is built with Key-value pairs.

SAM

Drivers

You hear a lot of talk about drivers in the Windows ecosystem, but not in Linux. That is because in Linux the drivers are open-sourced and included in the kernel, for most part. These drivers might be produced by nice programmers or they could be developed by the hardware-producer themselves. That's why it is so easy and fast to install new hardware on Linux. If it is compatible that is. Drivers are software lets the OS communicate with the hardware. Like networks cards, graphics card, printers. To list all the drivers on the machine use the following command:

```
driverquery
```

This can we good to know since drivers can contains vulnerabilities that can be used for priv-esc. Check out the chapter on that.

IIS - Windows web server

IIS stands for Internet Information Services (before it was Internet Information Server).

The software is usually includede in most Windows versions, except for the home editions. The IIS version usually corresponds to the OS version. There is a new IIS version for every new OS, in general.

By default IIS 5.1 and earlier run websites in a single process running the context of the System account

ASP

Activ server pages is the scripting environment for IIS. ASP render the content on the server side. The scripting languages that are supported are: VBScript, JScript and PerlScript.

Important files and stuff

SAM key

File types

In windows file-ending are important.

BAT

`.bat`-files are the windows equivalent to bash-scripts

In order to write a batch-script you open up an editor and then just write your commands. And then you save it as blabla.bat. And make sure you don't save it as a text file.

Then you just run the script from the cmd

DLL - Dynamic Link Library

A DLL file is a library that is used for one or more program. It is a binary-file but it is not executable in itself, but it contains code that the executable calls. It is used to modularize the code of a program.

In the windows operating system DLL files are shared among different applications. For example, the dll `Comdlg32` is used to create dialog boxes. So different applications can invoke this library to easily create a dialog box. This promotes code reuse.

So an application may use the standard windows DLL-files, but it may also bring its own DLL-files.

So if one DLL-file is missing for a program a certain module might not work. As most Windows-users have sometime experienced.

LIB

Lib is a bit like DLL, it is a library. But it is not dynamic as DLL. So lib-files are linked on compile-time. While dll-files are linked in run-time. Since lib-files are compiled into the executable you never see it (unless you are developing of course). But since DLL-files are dynamically loaded at run-time they are still around for the user to see.

References

http://compudyne.net/post08152012/ http://www.r00tsec.com/2012/11/howto-manual-pentest-windows-cheatsheet.html